

Companies learned many important lessons from the tragedies of September 11. Any corporate secretary reliant on old-fashioned, standalone minute books or those with an insubstantial document retention policy in place had to seriously rethink their disaster and minute-taking strategies.

An American Society of Corporate Secretaries publication, *Corporate minutes: a monograph for the corporate secretary*, points out that 'practical issues related to storing minute books should bridge between a company's document retention policies and disaster recovery plans.'

And there is a broad range of materials to be considered, including meeting notices, agendas, materials distributed to directors in advance of a meeting, reports and presentations made at a meeting, minutes in approved form and post-meeting communications.

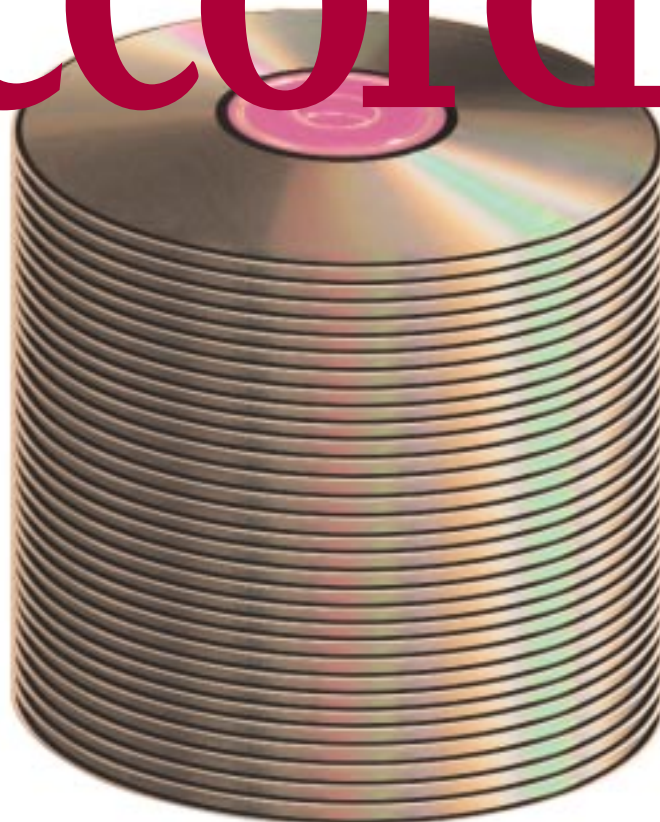
A basic retention policy and procedure means identifying why each item is being retained. Some of the possible reasons for doing so include legal compliance – simply following the advice of lawyers or other advisors – or for historic or archival objectives.

Just how effectively these methods are put into practice is summed up by Quimby Mills, formerly of data software provider 80-20 Software. 'The issue for us is not just that companies keep their minutes safe, but that they transfer all processes surrounding board and executive meetings to an electronic format that allows easy transportation to another location for safekeeping, as well as having the benefit

The potential for disaster has brought new impetus to minutes record-keeping and document disaster retention policies.

Adrian Holliday reports

On record



THE ROYAL APPROACH

Royal Bank of Canada's strategy for managing its corporate archive

Royal Bank of Canada's current minutes and appendices are printed on acid-free, archival quality paper and locked in fireproof cabinets in a secure vault. Operational copies are stored in electronic format on a secure server protected by strict user access protocols, and the server is backed up regularly. Indeed, electronic versions of RBC's minutes date back to 1990.

Minutes prior to this date and appendices dated more than a year ago are housed in an off-site archive with humidity and temperature controls. All records are stored in acid-free folders and boxes. Part of the corporate secretary's contingency plan requires minutes and appendices to be microfilmed on an annual basis, with security copies put in various locations across Canada. Amazingly, boardroom minutes stretching back to 1869 – almost as old as Canada itself – have all been microfilmed.

of being available to executives at any time, no matter where they are.'

Ford's assistant corporate secretary, Peter Sherry Jr, is taking these goals very seriously. 'We do recognize the security/preservation issue and the vulnerability of a single set of hard copy materials. This issue has risen in importance since September 11 and we're specifically addressing board and committee minutes and documents as part of an overall business continuity review,' he says.

So far much of the worry over document retention has been pinned against the grim backdrop of 9/11, a point not lost on Doug McCartney of corporate software provider Two-Step. 'Sure, it may be another

September 11 that could bring disaster, but it also could be an office closed because of an anthrax attack, a fire or a flood – or even documents just being plain lost,’ he says candidly. McCartney adds that there are hardly any public companies today that have not realized the critical importance of their historical records data: ‘We’ve seen a dramatic interest in the idea of a centralized database for key information and scanning finalized documents.’

The whys of online storage

From a security point of view this may be laudably sensible, but having huge troves of important historical records, often stored off-site, isn’t necessarily good for easy access. This is where online storage of scanned or digital documents comes in to play. Stored documents online can be backed up and replicated securely at another location. ‘Information can be easily shared and secured,’ says McCartney. ‘All your critical information and final documents are safely stored online and instantly available in a secure database environment.’

Getting your hands dirty here is inevitable – both literally and figuratively. Carol Lynch is a contract administrator with Washington, DC-based internet provider Cogent Communications. Cogent set up its own document retention program three years ago, a good while before the awful events of autumn 2001 exerted their pressure on others to follow suit. At the time, Cogent started retaining older documents, entering them into a database as well as taking hard copies off-site.

‘It was a tremendous amount of extra work,’ Lynch recalls. ‘Our priority was to look at the whole picture. Now all our contracts and minutes of meetings are scanned and all the originals get sent off-site to secure storage. Also, our network now gets backed up every night.’

Lynch still has her work cut out for her. A lot of paper documents like real estate contract agreements with partners need to be recorded and entered into a database. ‘When a contract is written, our people may need to refer back to the original. I scan all the documents so every single person doesn’t have to hold their own file. Then I put the original documents into boxes which get bar-coded. When around ten boxes of hard copies are ready to go they’re taken off to storage.’

‘Weaning people off their own file systems and getting them to store documents centrally will help immensely,’ says software expert Mills. ‘Changing employee habits while getting them used to a new system is the challenge – but one that the long-term benefits far outweigh.’

Security question

Nevertheless, even when a system is established – with full failsafe precautions bolted into position – there’s always the delicate issue of

combining security with access. In other words, says Nigel Blumenthal of corporate secretary software firm GK Holland & Associates, an access policy needs to be built *before* designing a software backup infrastructure around it.

‘Some corporate secretaries are uncomfortable with keeping records on a corporate network because of the possibility of unauthorized eyes seeing something they shouldn’t,’ Blumenthal observes.

‘However,’ he continues, ‘if your company has a properly organized corporate network, with a knowledgeable system administrator, competent security policies and a good firewall, you really should not worry. It’s more likely, for instance, that your computer’s hard drive will fail, or that you will get an e-mail virus that will destroy some files. If your minutes files are stored only on your own machine’s C drive, which is not usually backed up, you’re vulnerable to these risks.’

Those who adopt a solid minute documentation retention policy may find unexpected benefits. This was the case for Cogent, as corporate secretary Ried Zulager explains: ‘We saw it as an additional business opportunity. One of our businesses is moving data banks through our high-speed internet data services. So for other companies also needing to move large amounts of data online, we could market our product especially for them.’

Ready for scrutiny?

Corporate accounts and boardroom minutes have certainly come under closer public scrutiny in recent times. Getting rated by Institutional Shareholder Services or GovernanceMetrics, which evaluate corporate governance, doesn’t promise to make life any easier. As SEC commissioner Cynthia Glassman noted in a speech to ASCS members last September, ‘Corporate representatives are fiduciaries...They must often subjugate their own interests to the duties and obligations they owe to act in the best interest of their stakeholders.’

Best practice is demanding, but gritting your teeth and making sure your document retention plans meet expected standards should, as you progress, get easier. Zulager says changes to Cogent’s procedures have become so institutionalized they’re just part of normal business.

However, McCartney fires a warning salvo toward any company that delays: ‘The key is planning. Unless your documents are on the computer system before something bad happens, there is no way to get them back. Then they’re truly gone.’

UPGRADING BACKUP

- Keep minutes on a networked drive to allow for regular backup by IT staff
- Investigate costs and security issues for off-site storage of important documents
- Standardize the electronic format you use for documents
- Consider text indexing for easier information retrieval
- Advances in technology often render your archives unreadable (anyone still got a eight-track player?). Allow for this in your budgeting